Submit the completed PIA to
Privacy's SharePoint Customer Center

U.S. Speaker Program

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Tracker II

(b) Bureau: International Information Programs

(c) System acronym: TRKR II

(d) iMatrix Asset ID Number: 5189

(e) Reason for performing PIA: Align current PIA which expires Oct 2016, with in-process security assessment for ATO

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
In-process independent security assessment with IA for triennial ATO

(c) Describe the purpose of the system:
Tracker II is a central data repository for the U.S. Speaker Program managed by the Bureau of International Information Programs (IIP). Each year, the U.S. Speaker Program organizes approximately 650 traveling speaker and virtual interactive outreach programs in cooperation with Department of State field posts worldwide. These programs enable U.S. citizen experts to engage foreign publics in one or more countries abroad through speeches, lectures, consultations, workshops, seminars, and media

interviews. Major components of the U.S. Speaker Program include traveling programs and virtual interactive programs.

1. Traveling Speakers - Bringing an expert from the United States to speak to foreign audiences is a compelling way for field posts to support U.S. foreign policy, and communicate with foreign audiences about American society, institutions and culture.
2. Virtual Interactive Speaker Programs - IIP engages key foreign audiences through live interactive program platforms, including videoconferences, web chats and social media.

The Tracker II system stores contact information and biographical data/ curricula vitae on participating and potential U.S. Speakers. It is also a repository for program requests, significant communications with speakers and field posts, and evaluations for all traveling and virtual U.S. Speaker programs. The system captures program details, calculates and summarizes costs, and produces a tasking document that is e-mailed to the grantee organization that is responsible for logistical aspects of program administration (including travel bookings and ticketing, funding disbursement and passport/visa arrangements). It provides a business workflow for speaker projects, tracks program status, and monitors funding allocations and expenditures on a field post, regional and global basis. The system produces critical statistical reports on programs and budget. Tracker II is a closed accounting system, with manual re-entries into the U.S. Department of State's Global Financial Management System.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The following are elements of PII collected and maintained in Tracker II on individuals who are not U.S. government employees and who are participating as speakers or presenters in the International Information Programs (IIP) U.S. Speaker Program:

- Name of Speaker
- Date of birth
- Place of birth *
- Gender
- Address
- Telephone, cell, fax numbers
- Social Security number *
- Passport number *
- Visa numbers *
- Education
- Financial transactions *

NOTE * - Elements listed immediately above and listed below marked with * indicate PII that are no longer collected for non-U.S. Government employees. However, until such time that those elements are archived to NARA in accordance with published records requirements, they are still maintained in the backend database but not accessible through the front-end Tracker II system application.

The following are elements of PII collected and maintained in Tracker II only on individuals who are U.S. government employees and who are participating as speakers or presenters in the International Information Programs (IIP) U.S. Speaker Program:

- Name of Speaker
- Date of birth
- Place of birth *
- Gender
- Address
- Telephone, cell, fax numbers
- Social Security number *
- Passport number *
- Visa numbers *
- Education
- Financial transactions *

Outside the system, the Automated Clearing House (ACH) Vendor / Misc Payment Enrollment Form (SF3881) is completed with the U.S. government employee speaker’s contact information and social security number, as well as the their bank routing number, account number, contact information. This data is required for the U.S. government employee speaker’s Department of State Travel Authorization. The Speaker faxes the form or phones in the information to the U.S. Speaker Program which in turn sends the Form via Outlook to GFSC Charleston who uses the data to assign a vendor code to the U.S. government employee. The U.S. Speaker Program staff, after receiving the vendor code, then destroys the ACH Vendor Form and information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (Smith-Mundt);
- United States Information and Educational Exchange Act of 1948, as amended;
- 22 U.S.C. 2451-58 Fulbright-Hays Mutual Educational and Cultural Exchange Act of 1961, as amended;
- 22 U.S.C. 2651 a (Organization of the Department of State); and
- 22 U.S.C. 3921 (Management of the Foreign Service).

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: STATE-40 Employee Contact Records
- SORN publication date: November 2, 2010
-
- SORN Name and Number: STATE-65 Speaker/Specialist Program Records
- SORN publication date: December 10, 2009

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-37-010-03
- Length of time the information is retained in the system: All Tracker II (electronic) data files are TEMPORARY. For Biography Files - Cut off on the last update date timestamp. Destroy/delete when 50 years old. For all other Files - Cut off at the end of the fiscal year when the project ends. Destroy/delete when 50 years old.
- Type of information retained in the system:
  Biographic data on U.S. Speakers (or potential U.S. Speakers) and U.S. Speaker programs data.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No

- If yes, under what authorization?
NOTE: The U.S. Speaker Program no longer collects SSNs for retention in the Tracker II system. However, until such time that Tracker II electronic records with SSNs are destroyed in accordance with published records requirements, they are still maintained in

the backend database but not accessible through the front-end Tracker II system application.

(c) How is the information collected?

Data is collected directly from the record subjects. Additional data may be collected from publicly available information on the internet and through media reports. The U.S. Speaker Program staff use the internet to obtain bios, view papers, interviews, articles written by potential speakers, and lectures on YouTube. This information is also provided directly by the program participants.

For U.S. Government employees only, banking and other PII is obtained over the phone by the U.S. Speaker Program staff, or the grantee faxes/emails a completed questionnaire back to the International Information Programs (IIP) program officer.

All collected data is manually entered by the International Information Programs staff.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☒ Other

- If you did not select “Department-owned equipment,” please specify.

The grantee organization that is responsible for logistical aspects of program administration (including travel bookings and ticketing, funding disbursement and passport/visa arrangements) for non-U.S. government Speakers.

(e) What process is used to determine if the information is accurate?

Information collected directly from the record subject is presumed to be accurate. The contact information about an individual is collected from Department of State records and interviews with the subject individual.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The U.S. Speaker Program Officer confirms biographical and contact information for program participants prior to each program.

(g) Does the system use information from commercial sources? Is the information publicly available?

Data may be collected from publicly available information on the internet and through media reports. The U.S. Speaker and Specialist Program staff use the internet to obtain bios, read papers, interviews, and articles written by potential speakers, and to look at lectures on YouTube.

The U.S. Office of Personnel Management provides per diem and travel rates for U.S. Government employees.

(h) Is notice provided to the individual prior to the collection of his or her information?

A Privacy Act Statement is available for those individuals that provide this information by form, and notice is also given through System of Records Notices State-65 and State-40.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

The individual may decline to provide the required information; however, for the IIP Speaker and Specialist Program, such actions may prevent individuals from participating in that Program.

- If no, why are individuals not allowed to provide consent?

Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

A potential privacy risk involves unauthorized access to a Speaker's name, address, date of birth and biographical information. This risk is mitigated by hosting the Tracker II system and data only on the Department of State's intranet and not making that system and data available via the internet. This hosting restriction lessens the PII data exposure to only Department employees who must first be authorized to access the Department's intranet and then only to those whose role and need-to-know require them to be granted access by the system owner.

For Tracker II, information collected and maintained is the minimum amount of information necessary to fulfill IIP's statutorily mandated U.S. Speaker Program. The information is required to draft itineraries, plan and program Speaker activities and manage financial accounts. Data is checked for accuracy as submitted by the record subject and is verified against Department Records where appropriate.

For Tracker II, social security number, passport number and visa number are no longer collected in the system as the U.S. Speaker Program has initiated a new component to administer logistics. Travel and funding disbursement are now administered by the grantee organization World Learning, Inc. under a Cooperative Agreement.

5. Use of information

(a) What is/are the intended use(s) for the information?

For Tracker II, the information is required to draft itineraries, plan and program Speaker activities and manage financial accounts.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. Tracker II entirely supports the U.S. Speaker Program. The Program staff rely entirely on the Tracker II system to manage speaking programs.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

Click here to enter text.

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internally, the Tracker II information is shared with U.S. Department of State's overseas Posts that requested the program.

Externally, the Tracker II information is shared with World Learning and Seven Corners, Inc.

(b) What information will be shared?

Data shared with overseas Posts include the individual's name, biography, travel itinerary and email address. No passport, visa or social security numbers are shared.

Externally, World Learning is provided the individual's name, address, telephone number, email address and proposed travel itinerary, while Seven Corners, Inc. is provided the Speaker's name and date of birth.

(c) What is the purpose for sharing the information?

Internally, the purpose of sharing the information with overseas Posts that request the Speaker Program is to enable them to prepare for the program.

Externally, the Tracker II information is shared with World Learning to process visas, tickets and payments required by Speakers for their overseas travel. Information is shared with Seven Corners, Inc. in order to provide travel accident and sickness insurance during a program

(d) The information to be shared is transmitted or disclosed by what methods?

Internally, with U.S. Department of State's overseas Posts that request the Speaker Program, the information shared is via the Department Outlook email system.

If a Country Clearance is requested, it comes from the U.S. Speaker Program staff in Washington, DC to the Post to ensure that the Speaker has permission to enter the country under Embassy auspices. This communication is outside and separate from the Tracker II System. The Speaker staff enters the request in eCountry Clearance, a separate system on the Department of State's intranet.

For U.S. government employee travel, the U.S. Speaker Program staff completes the Automated Clearing House Vendor / Miscellaneous Payment Enrollment Form (ACH) with the speaker's contact and banking information and fax or email via Department of State's intranet, the form to the Global Financial Services Center (GFSC) in Charleston, SC facility. The original form is shredded once a vendor code is provided by GFSC Charleston. GFSC provides a discrete vendor code for each Speaker, which is in turn entered into Tracker II.

This ACH form is not generated from Tracker II. The Charleston Center processes the form and initiates payment to the speaker's account by entering the required information into the Department's Global Financial Management System (GFMS).

Externally, information is shared with World Learning, Inc. and Seven Corners, Inc. via phone calls, emails and faxes. Additionally, travel insurance enrollment data is shared with Seven Corners with manual input into State Department's COINS system. All communication is transmitted via secure U.S. Department of State communication channels.

(e) What safeguards are in place for each internal or external sharing arrangement?

For internal sharing, Tracker II is internal to the Department of State. The public does not have direct access to any of the systems. All communication is transmitted via secure U.S. Department of State communication channels.

When shared within the Department, all information is used in accordance with Tracker II's stated authority and purpose. Risks to privacy are mitigated by granting explicit access only to authorized persons within the Department.

For external sharing, Tracker II risks to privacy are mitigated by limited access to and release of personal information on a need-to-know basis to World Learning, Inc. and Seven Corners, Inc. Also, there is no direct electronic interface between the external vendors and the Tracker II system, or the COINS system and the Tracker II system.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

For sharing of information internally, a potential risk to privacy from internal sharing arises when employees assume they are, by default, authorized to access any privacy information they want if the hosting agency is authorized to process the information. However, access to privacy information is restricted not only to the agency managing the U.S. Speaker Program, but also to only those employees whose role is explicitly granted authorization to access and, if necessary, process privacy information.

For sharing of information externally, one runs the potential risk of having less control over the environment than if privacy information were restricted to a limited intranet and within defined physical boundaries. By sharing privacy information externally, the external entity may accidentally or intentionally share the information with others within their business environment that are not explicitly granted authorization to access the information.

To mitigate any breaches of PII, the Department of State has a cooperative agreement with World Learning, Inc. and a contract with Seven Corners, Inc.

For Tracker II, external sharing of information, as vendors of the United States government, employees of both companies maintain a government security clearance. Information is only released on a need-to-know basis to World Learning, Inc. and Seven Corners, Inc. under a statutory or other lawful authority to use and maintain such information.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals who wish to gain access to records pertaining to themselves should write to the Director, Office of Information Programs and Services; Department of State; SA-2; 515 22nd Street NW; Washington, DC 20522-6001. The individual must specify that they wish the Cultural Property Advisory Committee Records to be checked. At a minimum, the individual should include: Name; date and place of birth; social security number; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record, and the approximate dates which give the individual cause to believe that the Office of International Information Programs has records pertaining to them.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals who wish to amend records pertaining to themselves should write to the Director, Office of Information Programs and Services; Department of State; SA-2; 515 22nd Street NW; Washington, DC 20522-6001. The individual must specify that they wish the Cultural Property Advisory Committee Records to be checked. At a minimum, the individual should include: Name; date and place of birth; social security number; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record, and the approximate dates which give the individual cause to believe that the Office of International Information Programs has records pertaining to them.

A privacy risk associated with notification and redress can potentially occur when a Speaker has a change in his or her contact or banking information and does not communicate that change to the Department's U.S. Speaker staff. This can potentially cause the Speaker to not be paid per the travel authorization.

To mitigate these risks, Speaker Program Officers and Coordinators keep the Speaker informed from the beginning of communications that the collected information provided about and by the Speaker is maintained in the U.S. Speakers Program system called Tracker II. The staff also reminds the Speaker that if the Speaker's provided information should change during the course of the engagement, that the Speaker must contact the respective Program staff to update the information.

Speakers can contact their respective Program Officer or the Bureau of International Information Programs to ask what is recorded about them and request that information be amended if they believe it to be incorrect. The notice is reasonable and adequate in relationship to the system's purpose and use.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

During program engagement, Speaker Program staff communicate with the Speaker about procedures to correct their information. Also, notice is provided to individuals as part of the Grant Award Letter. Furthermore, notification is provided to the public via System of Records Notices State-65 and State-40.

8. Security Controls

(a) How is the information in the system secured?

Tracker II is internal to the Department of State with no access by the public. It is hosted on the Department's internal network and it has no direct electronic interface with external vendors.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Access to Tracker II is restricted to Department of State personnel that are approved to use the Department's intranet.

For the Tracker II system, the system functional administrators determine, on a case by case basis, who in the respective office staff is authorized to access the system and at what level. The level of access and capabilities permitted are restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records.

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology". Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Inactive accounts on the Department of State's internal network are defined by 5 FAM 828.1 as over 90 days of inactivity unless, per 5 FAM 828.2, there is an approved Special Circumstance where the account can be unused for up to 180 days of inactivity before it is subject to deletion. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. The assessment and authorization process independently verifies and validates the application system security controls. Administrative procedures, including independent security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system.

(d) Explain the privacy training provided to authorized users of the system.
Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security. Additionally, all Department direct hires and locally employed staff (LES) must pass PA-459, a course entitled Protecting Personally Identifiable Information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
Authentication to the Tracker II system is enabled via Single Sign-on to the Department's internal network.

(f) How were the security measures above influenced by the type of information collected?
Tracker II must comply with the Department's Moderate risk security controls as a result of its collection of PII.

9. Data Access

(a) Who has access to data in the system?
Access to Tracker II is restricted to Department of State personnel that are approved to use the Department's intranet and who are authorized to access the system in support of the U.S. Speaker Program.

(b) How is access to data in the system determined?
Access to data in Tracker II, and at what level, is determined and approved by system functional administrators, on a case by case basis, in consultation with the Director and/or Deputy Director of the U.S. Speaker Program.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Administrative procedures, including independent security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system. The level of access and capabilities permitted are restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records. The separation of roles with different access privileges is in accordance with NIST Special Publication 800-53.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

There is no placement of personally identifiable information (PII) on portable computers. Authorized system users who telecommute can only access the system through the Department of State's secure access using the Global OpenNet remote access software package with two-factor authentication where one of the factors is provided by a RSA soft/hard token with a use-once password

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology". Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

Department of State system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through Diplomatic Security.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of State systems and security. Contracts are reviewed upon renewal by management and contract personnel who are experts in such matters.

Version History

V1 (September 2013) – Original Version

V1.1 (January 2016) – Updated header to reflect that users should submit completed PIAs to the Privacy Division's SharePoint Customer Center, instead of emailing it to PIATeam@state.gov. Also, fixed section 8's broken text field.

V1.2 (March 2016) - Updated current PIA into the new PIA template required for approval. Updated IIP contacts due to change in management. Identified World Leaning as the external Department of State vendor processing travel arrangements for non-U.S. government employees.